
Index

128-bit encryption, 32

A

access between corporate locations
 configuring and securing VPNs,
 360–365

 configuring Windows 2000 as
 router, 345–360

 partner organization access,
 365–367

 security risks, 342

Access Control Entry (ACE),
 67, 81, 95

Access Control Lists. *See* ACLs

access permissions (table), 76

access to information, security
 risks and, 3

access to internal network, 8

access tokens
 defined, 95
 described, 66

access to network services, 6

access to network traffic, security
 risks and, 4

accessing resources on Windows
 2000 network, 65–70

account lockout
 policy, 126
 remote access, 314

account policies
 managing, 125–128
 testing, 164

ACE (Access Control Entry),
 67, 81, 95

ACLs (Access Control Lists)
 assigning ACEs to, 81
 defined, 95
 described, 67

 editing for DNS zones, 228, 229
 Registry (fig.), 83

Active Directory

 account policy management,
 125–128

 administrative task delegation,
 128–139

 advantage over Windows NT, 40
 built-in groups, rights (table), 142
 components, 110

 converting zones to, 227

 creating IPSec policies, 285

 designing structure of, 115–117
 DNS, reliance on, 220

 domains, 111

 forests, 112

 group policy implementation,
 144–155

 implementing security groups,
 139–144

 integrated zone, 221, 222, 256

 introduction, 109

 managing account policies,
 125–128

 organizational units (OUs), 113
 schema defined, 156

 securing, 116–124

 sites described, 114

 structure and trusts (fig.), 112

 Tree, 156

 user account use, 170

 vs. public key infrastructure, 170

Active Directory Tree defined, 156

Active Directory Users container
 (fig.), 143

Add New Hardware Wizard, 296

administering Group Policy
 inheritance, 151

administration, network, 45, 251

administrative rights, security and, 5

administrative tasks, delegating in
 Active Directory, 128

Administrators group, delegation
 control, 137

Adminpak.msi, 132

AH (Authentication Header
 Protocol)

 defined, 289

 described, 272–274

anti-virus programs

 corporate administration of, 45

 e-mail, 7, 380

 Internet access, 393

Apcompat.exe, 249

API, Extensible Authentication
 Protocol (EAP), 309

Apple Talk protocol, 297, 345

application-level security, 395

Application server mode, 239, 256

application support, PKI, 177

applications

 installing automatically,
 remotely, 231

 network, evaluating security
 needs, 49

 that use PKI technology, 177

attacks

 corporate networks, 8–9

 DoS. *See* DoS attacks

 e-mail virus, 7

 external security risks, 8

 firewall, 390

 IP spoofing, 380

 man-in-the-middle, 4, 5

 out-of-band, 390

 social engineering, 315

- auditing, 86, 96
- authentication
 - certificate-based, 63, 64
 - client, defined, 209
 - configuring options for remote access clients, 312
 - configuring remote access, 308–317
 - down-level client, 63
 - evaluating corporate security, 47
 - Kerberos process (fig.), 59, 60
 - mutual, 359, 369
 - network, 58
 - NTLM, 62
 - PKI process, 172
 - remote access, 65
 - server, defined, 210
 - SMB signing, 266
 - UNIX, 251–252
 - user, 58–65
 - user resource, WAN connections, 344
- Authentication Header Protocol.
See AH
- Authentication Service defined, 96
- Authenticode, digitally signed content, 180

B

- back-to-back DMZ, use described, 392
- Bandwidth Allocation Protocol (BAP)
 - configuring with multilink properties, 300
 - defined, 331
- Basicdc.inf, Basicsv.inf, Basicwk.inf, 249
- best practices
 - access between corporate locations, 368
 - Active Directory design, 155
 - implementing PKI, 207–208

- network communications security, 287–288
- PKI planning, implementation, 207
- securing network resources, 93–94
- securing network services, 254–255
- securing remote access, 330
- biometric systems, 58
- blocking Group Policy inheritance, 152
- bulk encryption key, 210
- business model, 22, 36
- business processes, 28–31
- business-to-business (B2B) communications, 365

C

- CA (Certificate Authority). *See also* CAs
 - enterprise root, 184
 - hierarchy, 183, 209
 - root, defined, 209
 - root certificate (fig.), 176
 - standalone, subordinate, 185, 210
- callbacks
 - configuring options, 312, 313
 - defined, 331
- caller IDs, 313, 331
- card readers, 180
- CAs (Certificate Authorities). *See also* CA
 - authentication infrastructure, 64
 - certificate server hierarchy, 182
 - defined, 96, 209
 - described, structure, 174
 - installing, 188
 - integration with third-party, 205
 - managing group policy settings, 198
 - PKI process described, 173
 - standalone, 185
- subordinate root, 185
- verification process, 175
- case projects
 - Fleetwood Credit Union
 - security risk evaluation, 20
 - connecting company locations, 375
 - group policy
 - implementation, 167
 - Internet security, 411
 - PKI solution, 217
 - remote access, 339
 - securing network communications, 294
 - securing server resources, 108
 - terminal service deployment, 264
- Southdale Property Management
 - access by partner organizations, 375
 - DNS, Terminal Services, 263
 - LAN security concerns, 19
 - PKI investigation, 217
 - remote access
 - implementation, 339
 - securing network communications, 294
 - securing server resources, 107
 - setting password policies, 167
 - speeding access to Internet, 411
 - Technical Consultants, security planning, 56
- certificate-based authentication
 - choosing method of assignment, 193
 - configuring servers to use, 191
 - cross, 184
 - described, 63, 64
 - mapping user accounts to, 199–201

- requesting from a Certificate Server (fig.), 202
 - revocation of, 197
 - Certificate Server, 170
 - and CA hierarchy, 182–183
 - client implementation, 201–205
 - described, 209
 - implementation, 188–199
 - installing, 188–191
 - certificate server hierarchy and type, 182, 184
 - certificates. *See* digital certificates
 - Certificates snap-in, requesting, managing certificates with, 204
 - certificate templates available in Windows 2000 (table), 187
 - Certification, MCSE, exam objectives, Appendix A
 - Certification Authority. *See* CA, CAs
 - certification requests
 - configuring advanced settings (fig.), 203
 - managing, 196
 - Challenge Handshake Authentication Protocol (CHAP), 65, 310
 - change-control policies, corporate, 46
 - CHAP (Challenge Handshake Authentication Protocol), 65, 310
 - child domains defined, 156
 - Cipher command line tool, 94
 - clear text, and SMTP, 4, 10
 - client authentication defined, 209
 - clients, prestaged, 257
 - Client Services for Netware, 253
 - Code Red Worm, 379
 - commands
 - choosing for taskpad (fig.), 136
 - secedit.exe, 124
 - communities, SNMP, 245
 - company networks, limiting access to, 366
 - Compatws.inf, 249
 - Computer Local group, 156
 - computers
 - information exchange between, using IPsec, 277
 - theft of, 3
 - confidentiality of data over WAN connections, 344
 - configuring
 - client proxy settings (fig.), 401
 - dial-up servers, 296
 - firewalls, 385–386
 - IAS, 326
 - ICS, 382
 - Internet clients, 396–401
 - Internet Explorer Content Advisor (fig.), 400
 - IP filter properties (fig.), 280
 - network options for dial-up clients (fig.), 303
 - remote access clients, 300
 - remote access policies, 319
 - RIS, 232, 237
 - router-based packet filter (fig.), 358
 - router options, 345–348
 - RRAS server authentication method (fig.), 311
 - RRAS to use IAS (fig.), 329
 - security policy setting (fig.), 88
 - SMB security, 266–271
 - SNMP trap destinations (fig.), 247
 - taskpads, 133
 - VPN client, 307
 - VPN port settings (fig.), 306
 - VPNs, 360
 - containers, Group Policy, 146
 - Content Advisor, 399
 - control lists
 - access, 67
 - NTFS Access (fig.), 69
 - corporations, business model, 22
 - corporate locations
 - access between. *See* access between corporate locations
 - collecting information about, 41
 - encrypting traffic between, 10
 - securing access between, 341–367
 - securing data transmission, 365–366
 - corporate networks, hacking into, 8
 - corporations
 - business processes of, 28
 - change-control policies of, 46
 - corporate management model, 32
 - geographic scope, 31–32
 - growth strategies, 37
 - IT integration, 38
 - locations. *See* corporate locations
 - networking structures, services, 42–46
 - network security evaluation, 49
 - ownership and control, 23–24
 - privately owned, 25
 - products and services, 26, 28
 - public and private information, 29
 - relationships with other organizations, 35
 - security model, identifying current, 48
 - security planning components, 21–50
 - structure of publicly traded (fig.), 23
 - visions and goals, 36
 - Cpresult utility, 154
 - creating
 - Group Policies, 148
 - IP filters, 279
 - IPsec policy rules, 284
 - packet filter, 357
 - Registry configuration file, 269
 - security templates, 162, 250
-

- shared folders, 71, 102
- taskpads, 133
- trust paths, 184
- VPN connection (fig.), 304
- credentials
 - setting remote dial-up (fig.), 359
 - dial-in, dial-out, 356
- CRLs (certificate revocation lists)
 - defined, 209
 - publishing schedule, 197
- cross certificates, 184
- customizing MMC, 132
- D**
- DACLs (Discretionary Access Control Lists), 67, 96
- data encryption
 - and e-mail, 179
 - levels, 243
 - using private, public, session keys (fig.), 171
- data integrity, WAN connections, 344
- data recovery
 - certificates, 199
 - managing, 80
- DC Security.inf, 250
- decentralized IT administration model, 39
- decision-making process, corporate, 31
- Defltcdc.inf, Defltsv.inf, Deflwtwkk.inf, 248
- delegating administrative tasks, 128
- delegation, designing Active Directory for, 137
- Delegation of Administration Wizard, 138
- Delegation of Control Wizard, 131
- delegations, 156
- demand-dial
 - interface, adding, 373
 - securing VPN connection, 375

- demand-dial routers
 - configuring RRAS as, 351
 - defined, 369
- demand-dial routing, 347, 352
- demilitarized zone. *See* DMZ
- denial-of-service attack. *See* DoS attacks
- deploying IPSec policies, 284
- designing
 - Active Directory for
 - delegation, 137
 - certificate server hierarchy, 182
 - firewalls, 2
 - secure access to Internet, 377–395
 - secure networks, 11
- DHCP (Dynamic Host Configuration Protocol)
 - defined, 257
 - gathering information at corporate locations, 44
- DHCP servers
 - adding to DNSUpdateProxy group, 230–231
 - and IP addresses, 219
 - configuring to update DNS, 224
- dial-in profiles, configuring (table), 321
- dial out credentials, 356
- dial-up clients
 - configuring, 300
 - configuring network
 - connection type (fig.), 301
 - configuring network options for (fig.), 303
- dial-up connections and private network infrastructure, 342
- dial-up servers
 - configuring, 296
 - configuring IP addressing options, 299
- Digest Authentication, 65

- digital certificates
 - defined, 209
 - PKI process, 173
- digital signatures
 - and e-mail, 179
 - hash described, 172
 - purpose, 171
- Digital Subscriber Line (DSL), 304
- digitally signed content, 180
- directory service defined, 156
- Directory Services Client, down-level client authentication, 63
- Discretionary Access Control Lists (DACLs), 67, 96
- distributed model of IT administration, 39
- distribution groups, 139, 157
- DMZ (demilitarized zone)
 - back-to-back, 392, 404
 - defined, 404
 - described, 390
 - designing for corporations, 22
 - limiting access to resources using, 366
 - securing resources within (fig.), 367
 - three-horned firewall, 391
- DNS (Domain Naming Service)
 - configuring DHCP servers to update, 224
 - defined, 257
 - Dynamic, defined, 257
 - gathering information about networking services, 44
 - tab options (fig.), 225
- DNS servers
 - and DHCP servers, 219
 - securing installation, 222–223
 - zone types, 221–222
- DNS service described, 220
- DNSUpdateProxy security group described, 256

- properties (fig.), 231
- secure dynamic update
 - process, 230
- DNS zones
 - converting to be Active Directory integrated, 227
 - defined, 256
 - described, 221
- Domain Admins group, 5, 116
- Domain Controller, DNS and, 220
- domain local groups defined, 157
- Domain Naming Service. *See* DNS domains
- domains
 - child, defined, 156
 - defined, 157
 - root, defined, 157
- DoS attacks
 - bandwidth consumption (fig.), 7
 - defined, 13
 - described, 6
- down-level client authentication, 63
- drivers
 - IPSec, 277, 289
 - software, incompatibility with other components, 393
- DSL (Digital Subscriber Line), 304
- Dynamic DNS defined, 257
- Dynamic Host Configuration Protocol. *See* DHCP
- dynamic updates
 - DNS and, 223–224
 - process described, 229

E

- EAP (Extensible Authentication Protocol), 65, 309, 331
- e-commerce
 - authentication process, 172
 - certificate-based authentication, 63
- editing access control lists, 68
- EFS
 - data encryption, decryption, 181
 - defined, 96

- described, 78
- implementing, 79
- e-mail
 - evaluating corporate security needs, 47
 - secure, 179
 - virus-infected, 7, 380
- Encapsulating Security Payload (ESP), 274, 289
- Encrypted File System, EFS
- encrypting
 - file system, 78–81
 - traffic between corporate locations, 10
- encryption
 - 128-bit outside of N.America, 32
 - adjusting level in Terminal Services, 243
 - defined, 369
 - IP Security (IPSec), 181
 - over WAN connections, 359
 - public and private keys, 171
 - viewing settings with Cipher, 94
- Enterprise Admins group, 116
- enterprise CA defined, 209
- enterprise root CA, 184
- EPROM, 180
- erasable, programmable memory (EPROM), 180
- ESP (Encapsulating Security Payload), 274, 289
- event logs
 - filtering, 91, 92
 - managing, 89
 - and security templates, 119
- Events Properties dialog box (fig.), 91
- Event Viewer
 - auditing with, 86
 - on domain controller (fig.), 90
- Exam, MCSE Certification, Appendix A

- examples of shared and NTFS permissions (table), 77
- exporting IP Security policies, 286
- Extensible Authentication Protocol (EAP), 65

F

- file downloads, unauthorized, 393
- file resources, securing, 70–78
- file structures, designing for access, 70
- file systems, encrypting, 78–81
- filtering
 - event logs, 91, 92
 - Group Policy settings, 153
 - packet, 357, 369
- filters
 - IP, creating, 279
 - packet, defined, 405
- firewall attacks, 390
- firewall rules
 - allowing HTTP traffic (fig.), 387
 - described, 388, 404
- firewalls
 - configuring, 385
 - and corporate IT administrative model, 40
 - corporate security, 34
 - defined, 13, 404
 - described, 1
 - hackers circumventing, 8
 - IPSec packets and, 364
 - ISA Server 2000 as, 395
 - network security, 49
 - separating private networks from Internet, 386
 - static mapping configurations on (fig.), 389
 - three-horned DMZ, 391
 - usage reports and intrusion detection, 390
- Fleetwood Credit Union. *See* case projects

folders, creating shared, 71, 102
forests defined, 157
forward lookup zones, 221
FTP (File Transfer Protocol), 394

G

Gateway Services for Netware, 253
Generic Routing Encapsulation (GRE), 362, 369
Generic Routing Protocol (GRE), 362
geographic scope of security plans, 31
global catalogs defined, 157
global groups, 142, 157
globally unique identifier (GUID), 146, 235
GPOs (Group Policy Objects)
 creating, 166
 described, 146
GRE (Generic Routing Encapsulation), 362, 369
group policies. *See also* Group Policy
 conflicts between, 150
 creating, 148
 implementing for security, 144
 IPSec configuration, 278
 options for policy enforcement (table), 151
 Public Key Policies (fig.), 198
 SMB signing, 270
Group Policy. *See also* group policies
 administering inheritance of, 151
 assigning Account Policy to Active Directory, 119
 blocking inheritance (fig.), 152
 configuration options (table), 145
 defined, 157
 enabling, disabling settings (fig.), 149
 managing, 147
 no override option (fig.), 153

objects, 146
overview, 144
troubleshooting settings, 154

groups

 Computer Local, defined, 156
 default, built-in, 140
 distribution, 139, 157
 DNSUpdateProxy security, 256
 domain local, defined, 157
 Global, defined, 157
 local rights (table), 141
 security. *See* security groups
 Universal, defined, 157

GUID

 described, 146
 determining a computer's, 235

H

hackers, corporate networks and, 8
handshake, SSI, 178
hands-on projects
 adding demand-dial interface, 373
 company security plan design, 54–55
 configuring
 Certificate Services for smart card use, 215
 Content Advisor, 410
 NAT servers, 408
 Routing and Remote Access as router, 373
 RRAS as Network Address Translation server, 408
 RRAS as VPN server, 336
 creating
 custom MMC, 163
 custom MMC and adding security snap-in, 161
 security templates, 162
 user account permissions, 336
 User Certificate for encrypted e-mail, 216
 delegating administrative tasks, 164

DNS server configuration, updates, 261
installing Certificate Services, 214
IPSec policies, 293
researching company security needs, 54
revoking a certificate, 216
securing
 client web browser, 409
 resources in servers, 102
setup, system requirements, 17
SMB signing request, 292
testing account lockout policy, 164
hardware, requirements for hands-on projects, 17
hash described, 172
hierarchy, certificate server, 182
Hisecws.inf, Hisecdc.inf, 250
HKEY-LOCAL_MACHINE Registry key, 84, 314

I

IAS (Internet Authentication Service)
 adding RADIUS client to (fig.), 328
 administration tool, 327
 configuring (fig.), 327
 configuring as RADIUS server, 326
 configuring RRAS to use, 329
 defined, 331
 installing, 326
ICMP, Smurf program and, 7
ICS (Internet Connection Sharing)
 configuring, 382
 defined, 331, 404
 described, 381
 enabling (fig.), 383
identifying client certificate needs, 186
IEAK, 401, 405

- IIS (Internet Information Services)
 - basic security measures, 380
 - planning for security, 379
 - Certificate Wizard (fig.), 193, 194
 - IKE (Internet Key Exchange), 277, 289
 - images, using RIS to limit client access, 237
 - implementing
 - demilitarized zones, 390
 - EFS, 79
 - security groups, 139–144
 - incremental templates, 249
 - information
 - corporate public and private, 29
 - technology. *See* IT
 - inheritance
 - Group Policies, 150
 - permission, 129
 - installing
 - applications automatically, 231
 - Certificate Servers, 188–191
 - IAS, 326
 - SNMP service, 246
 - Terminal Services, 262
 - Windows 2000 Professional clients with RIS, 233
 - Windows 2000 Terminal Services, 239
 - insurance companies, business process at, 30
 - internal network, access to, 8
 - internal security risks, threats and, 2
 - international organizations
 - security plans, 31
 - Internet
 - analyzing exposed components, 379
 - firewall separating private network from (fig.), 386
 - securing internal network from, 378–385
 - usage policies, 401
 - Internet Authentication Service. *See* IAS
 - Internet clients, configuring, 396
 - Internet Connection Sharing. *See* ICS
 - Internet Control Protocol (ICMP), 7
 - Internet Engineering Task Force (IETF), 209
 - Internet Explorer Administration Kit (IEAK), 401
 - Internet Explorer Content Advisor, 399, 405
 - Internet Information Services. *See* IIS
 - Internet Key Exchange (IKE), 277
 - Internet Protocol Security. *See* IPSec
 - Internet security zone, 396
 - Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX), 345
 - IP addresses
 - assigning to client computers with RRAS (fig.), 298
 - configuring for RRAS, 348
 - configuring Windows 2000 not to register, 226
 - IP filters, 279, 281
 - IP spoofing attacks, 380
 - IPSec (Internet Protocol Security)
 - AH packet structure (fig.), 273
 - Authentication Header Protocol (AH), 272–274
 - authentication methods, 282
 - creating policies for Active Directory use, 285
 - defined, 13, 209, 289
 - deployment, 284
 - driver, 277, 289
 - Encapsulating Security Payload (ESP), 274
 - exporting policies, 286
 - hacker protection, 9
 - negotiation process (fig.), 278
 - policy creation, 283
 - printer security, 82
 - protecting network data, 181
 - securing network traffic using, 9, 271–288
 - and SMB signing, 266
 - Transport, Tunnel modes, 275–276
 - Tunnel mode, encrypting packets, 365
 - and Windows 2000, 277
 - IPX/SPX, 345
 - ISA Server 2000, 395
 - ISDN connections, 296
 - IT administrative structures, identifying, 39
 - IT infrastructure, corporate integration, 38
- K**
- KDC (Key Distribution Center)
 - defined, 96
 - Windows 2000, network security services, 59
 - Kerberos
 - authentication process (fig.), 60, 62
 - IPSec authentication, 282
 - network access control, 271
 - policy, 127
 - smart cards, using, 180
 - UNIX, 252
 - version 5, 96, 252
 - Windows 2000 and, 4
 - key, private. *See* private key
 - key, public. *See* public key
 - key, session. *See* session key
 - Key Distribution Center, 59, 96
-

L

L2F (Layer 2 Forwarding), 363
 L2TP (Layer Two Tunneling Protocol)
 protection against network sniffers, 223
 defined, 332, 369
 IPSec and, 182, 364
 and VPN, 305, 363
 L2TP/IPSec encapsulation structure (fig.), 364
 LAN network diagram (fig.), 42
 LAN-to-LAN configurations, 349
 laptops, corporate security evaluation, 48
 Layer 2 Forwarding (L2F), 363
 Layer Two Tunneling Protocol. *See* L2TP
 local file system security, 242
 local group rights (table), 141
 local Internet security zone, 397
 Local Security Settings (fig.), 120
 lockout
 account, 126
 remote access account, 314
 logon, interactive, 58
 logs, event. *See* event logs

M

Macintosh clients, accessing RRAS servers, 297
 management model, corporate, 32–34
 management rights, SNMP communities, 245
 managing
 account policies, 125
 administrative task delegation, 130
 certification requests, 196
 certification revocations, 197
 data recovery, 80
 event logs, 89
 group policies, 147

Group Policy settings for a CA, 198
 RIS servers, 235
 security groups, 143
 security risks, 11–12
 man-in-the-middle attacks, 4, 5
 mappings
 reverse proxy (static), 405
 static, 388, 389
 user accounts to certificates, 199–201
 MCSE Certification Exam objectives, Appendix A
 Melissa virus, 7
 memory, erasable, programmable (EPROM), 180
 message digest defined, 209
 messages
 authentication, 266
 sending to connected users, 73
 Microsoft Challenge Handshake Authentication Protocol. *See* MS-CHAP
 Microsoft Management Console. *See* MMC
 Microsoft Point-to-Point Encryption. *See* MPPE
 Microsoft Proxy 2.0, 395
 Microsoft Security Notification Service, 18, 379
 Microsoft Security Tools web site, 380
 Microsoft Services for UNIX version 2.0, 251
 MMC (Microsoft Management Console)
 customizing, 132
 Security Template snap-in, 118
 modems
 bypassing security with personal, 394
 choosing as demand dial interface (fig.), 354

detecting, connecting, 296
 and NAS, 324
 monitoring
 shared folder availability, 104
 shares, 73
 MPPE (Microsoft Point-to-Point Encryption)
 defined, 369
 VPN protocol, 362
 MS-CHAP (Microsoft Challenge Handshake Authentication Protocol)
 defined, 332
 described, 308
 Remote Access authentication (table) 65
 version 2, 309
 multilinking, 299
 mutual authentication, 359, 369

N

naming conventions, corporate security planning, 34
 NAS (Network Access Server)
 defined, 332
 described, 324
 NAT (Network Address Translation)
 described, using, 372–377
 features, 385
 internal hosts access Internet (fig.), 382
 servers, configuring using RRAS, 384
 used behind firewall, 287
 viewing Session Mappings table (fig.), 386
 NDS (Network Directory Service) 252
 Netware clients, securing network access to, 252
 network access, securing for Macintosh clients, 253–254

- Network Access Server. *See* NAS
 - network address translation.
 - See* NAT
 - network administration
 - collecting corporate information about, 45
 - tools, Remote Installation Services (RIS), 231
 - network authentication, 58
 - network cards, and IPSec negotiation process (fig.), 278
 - network communications
 - securing, 265–288
 - securing traffic with IPSec, 271–286
 - SMB signing, implementing, 266–271
 - Network Connection Wizard, 301
 - network diagrams
 - LAN sample (fig.), 42
 - WAN sample (fig.), 43
 - Network Files System (NFS) software, 251
 - networking
 - infrastructure, LAN diagram sample (fig.), 42
 - services, gathering information about, 44–45
 - networks
 - designing secure, 11
 - internal *See* internal networks, 8
 - network services
 - access to, DoS attacks and, 6
 - implementing
 - DNS and DHCP security, 220–231
 - RIS security, 231–238
 - secure access for nonMicrosoft clients, 250, 250–254
 - SNMP security, 244–247
 - terminal server security, 238–244
 - securing servers using security templates, 247–250
 - network traffic
 - access to, and security risks, 4
 - policies prohibiting outside connections, 271
 - NFS software, 251
 - nonMicrosoft clients, securing access for, 250–254
 - NOTEPAD.EXE, 106
 - Notssid.inf, 242, 250
 - NT file system, 3
 - NTFS (NT File System)
 - permissions, 5, 74–78, 96
 - NTLM authentication (Windows NT Lan Manager), 62, 96
 - nudity, filtering, 399
- O**
- Oakley logs, 288
 - OCFiles.inf, OCFilesw.inf, 250
 - Open Shortest Path First. *See* OSPF
 - organization chart, corporate, 34
 - organizational unit (OU)
 - defined, 157
 - OSPF (Open Shortest Path First)
 - defined, 369
 - described, 351
 - routing options, 345
 - out-of-band attacks, 390
 - overriding permission inheritance, 129
- P**
- packet filtering
 - defined, 369
 - described, 357, 387
 - packet filters
 - defined, 405
 - described, 387
 - packets, virus attacks and, 7
 - packet sniffers
 - access to network traffic, 4
 - defined, 3, 13
 - protecting against, 48
 - packet structures
 - IPSec AH (fig.), 273
 - IPSec ESP (fig.), 274
 - PAP (Password Authentication Protocol), 65, 310
 - partitions, NTFS, 5
 - Password Authentication Protocol (PAP), 65, 310
 - password policies
 - changing in a company, 11
 - managing accounts, 125
 - evaluating, 49
 - IT administrative model, 40
 - passwords, random generating device, 310
 - patches, security, 18, 379
 - path, trust. *See* trust paths
 - PDAs, evaluating corporate security needs, 47
 - performance, CPU, and SMB signing, 266
 - permission inheritance, 129
 - permissions
 - combined share and NTFS, 77
 - configuring Terminal Services connection (fig.), 242
 - inheriting, 129
 - managing in corporations, 34
 - NTFS, 74–78, 96
 - overriding inheritance of, 129
 - printer (table), 81
 - remote access policies, 317
 - remote access (table), 318
 - share, 70–74, 96
 - shared NTFS (table), 75
 - special access (table), 76
 - special Registry (table), 84
 - Permissions Entry dialog box (fig.), 76
 - Personal Digital Assistants, PDAs
 - PGP (Pretty Good Privacy)
 - described, 209
 - and secure e-mail, 180
-

- ping-of-death, 390
- PIN numbers, 310
- PKI (Public Key Infrastructure)
 - application support, 177
 - authentication, 164, 172
 - best practices, planning, 207
 - Certificate Authorities, 174, 205–206
 - Certificate Server client implementation, 201
 - certificates, 173
 - data encryption, 171
 - described, 13, 209
 - designing certificate server hierarchy, 182–184
 - digitally signed content, 180
 - digital signatures, 171
 - EFS (Encrypted File System), 181
 - IPSec (IP Security), 181, 282
 - mapping user accounts to certificates, 199
 - overview, 170
 - planning and implementing, 182–188
 - public, private keys, 170
 - smart card logon, 180
 - trust paths in (fig.), 177
 - vs. Active Directory, 170
 - Windows 2000 Certificate Server implementation, 188
- planning
 - best practices, 93–94
 - certificate server type, 184
 - remote access policies, 322
 - security, 21–50
- Point-to-Point Protocol (PPP), 300
- Point-to-Point Tunneling Protocol (PPTP), 223
- policies
 - account, assigning, 119
 - Account Lockout (table), 126
 - audit, 86
 - certificate, defining, 186
 - data recovery, 80
 - Internet usage, 401
 - Kerberos, 127
 - password, 125
 - remote access, 317–322
 - port numbers of network services, 388
 - ports, RRAS, viewing (fig.), 353
 - port scans, 390
 - PPP (Point-to-Point Protocol), 300
 - PPTP (Point-to-Point Tunneling Protocol)
 - defined, 370
 - protecting zone transfers, 223
 - VPN protocol, 362
 - prestaged clients defined, 257
 - Pretty Good Privacy (PGP), 180
 - principals, security, 66
 - printers
 - permissions (table), 81
 - security risks, 3
 - private keys
 - defined, 209
 - public key infrastructure and, 170
 - private network infrastructure, defined, 342
 - products and services, corporate, 27–28
 - profiles, configuring dial-in (fig.), 321
 - projects
 - case. *See* case projects
 - hands-on. *See* hands-on projects
 - Rhode Island College security plan, 55
 - properties, event log (fig.), 93
 - protocol-level security, 395
 - protocols. *See also specific protocol*
 - Apple Talk, 297
 - Authentication Header (AH), 272–274
 - Bandwidth Allocation Protocol (BAP), 331
 - Extensible Authentication (EAP), 309
 - Generic Routing Encapsulation (GRE), 362
 - Layer 2 Forwarding (L2F), 363
 - Layer 2 Transport Protocol (L2TP), 182, 332, 363
 - NTLM (NT Lan Manager), 62
 - OSPF (Open Shortest Path First), 351
 - Point-to-Point (PPP), 300
 - remote access (table), 65
 - Remote Desktop (RDP), 243
 - routing, 350, 370
 - VPN options, 361–365
 - proxy servers
 - client configurations, 400
 - defined, 405
 - described, 394
 - proxy services, implementing, 394
 - public key defined, 209
 - Public Key Infrastructure (PKI), 49
 - Public Key Policies, 198–199
 - public keys and public key infrastructure, 170
 - public network infrastructure, 343

R

 - RADIUS (Remote Authentication Dial-in User Service)
 - adding client to IAS (fig.), 328
 - complex server implementation (fig.), 325
 - defined, 332
 - introduction, 323
 - server implementation (fig.), 324
 - using IAS, 326
 - RAS (remote access service)
 - defined, 332
 - described, 295
 - points of network attacks, 9

- RDP (Remote Desktop Protocol)
 - defined, 257
 - described, 243
 - Terminal Services use of, 366
 - recovery agents, 78, 96
 - Recreational Software Advisory Council on the Internet (RSACi), 399
 - Registry
 - Access Control List (fig.), 83
 - configuration files, editing and deploying, 269
 - default setting, 85
 - editing SMB configuration settings (fig.), 267
 - HKEY_LOCAL_MACHINE key, 314–315
 - securing, 82–86
 - and security templates, 120
 - special permissions (table), 84
 - Registry Editor, modifying permissions in (fig.), 85
 - Relative Identifier (RID), 66
 - remote access
 - account lockout, 314
 - best practices, 330
 - callback options, 312
 - planning policies, 322
 - policies, 317–323
 - policy conditions, permissions, profile (table), 318
 - securing, 308–317
 - service. *See* RAS
 - unauthenticated, 310
 - user account administration, 316
 - remote access authentication, 65
 - remote access policies, defined, 332
 - remote access security, 241–242
 - remote access service. *See* RAS
 - Remote administration mode, 239, 257
 - remote application services, using Terminal Services for, 238
 - Remote Authentication Dial-in User Service. *See* RADIUS
 - Remote Desktop Protocol. *See* RDP
 - Remote Installation Services. *See* RIS
 - Request for Comment (RFC)
 - 1918, 381, 405
 - requests, certification, 196
 - resources, file , 70
 - restricted Web sites, 397
 - reverse proxy mappings
 - described, 388
 - Reverse Proxy (static) mappings, 405
 - revocation of certificates, 197
 - RFC specifications, 59, 381, 405
 - Rhode Island College security plan project, 55
 - RID (Relative Identifier), 66
 - RIP (Routing Information Protocol), 350, 370
 - RIS (Remote Installation Services)
 - defined, 257
 - described, 220
 - implementing, 231–238
 - TFTP role, 238
 - root CA
 - enterprise, 184
 - certificate (fig.), 176
 - and certificate authorities, 175
 - defined, 209
 - root domains defined, 157
 - routers
 - configuring Windows 2000 as, 345
 - defined, 370
 - demand–dial, defined, 369
 - described, 345
 - Routing and Remote Access Service. *See* RRAS
 - Routing Information Protocol (RIP), 350, 370
 - routing protocols, 350, 370
 - routing tables, 349, 370
 - RRAS (Routing and Remote Access Service)
 - configuration options (fig.), 297, 347
 - configuring
 - as demand–dial router, 351
 - as router (fig.), 346
 - IP address allocation for (fig.), 348
 - IP addressing (fig.), 299
 - NAT server using, 384
 - to assign IP addresses to clients, 298
 - to use IAS, 329
 - VPN server, 305
 - defined, 332, 370
 - described, 344–345
 - servers, configuring authentication method, 311
 - Setup Wizard, 346
 - unauthenticated access, 310
 - viewing ports (fig.), 353
 - RSACi (Recreational Software Advisory Council on the Internet), 399
- ## S
- SA (Security Association), 277, 289
 - SACLs (System Access Control Lists), 67, 96
 - schemas, Active Directory, 156
 - screen subnet, 390
 - screened subnets, 404
 - secdit.exe, 124, 157
 - secure access, securing for nonMicrosoft clients, 250–254
 - secure dynamic updates, 257
 - secure e-mail, 179
 - secure Internet access, designing, 369
 - Secure Sockets Layer. *See* SSL
 - secure updates, 227–229
-

- secure Web sites, 178
 - Securedc.inf, 249
 - Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3, 180, 210
 - Securews.inf, 249
 - securing
 - access between corporate locations, 341–367
 - Active Directory, 116
 - data transmissions between locations, 365
 - dynamic updates to DNS, 226–231
 - file resources, 70–78
 - network access to Netware clients, 525
 - network communications, 265–288
 - network services, 219–255
 - printers, 81
 - Registry, 82–86
 - remote access, 308–317
 - remote user access, 295–329
 - RIS, 234
 - SNMP transmissions, 247
 - Terminal Services, 241
 - user access to Internet, 393–403
 - VPNs, 360
 - Windows 2000 router, 357
 - security
 - account policy implications, 127
 - application-level and protocol-level, 395
 - bypassing using personal modems, 394
 - local file system, 241
 - printer, 81–82
 - reports, 390
 - SNMP, 244–247
 - transmission, 243–244
 - Security Analysis configuration screen (fig.), 123
 - Security and Configuration tool set, 117, 157
 - Security Association. *See* SA
 - Security Configuration and Analysis utility, 121, 122
 - security groups
 - defined, 157
 - implementing, 139–144
 - managing, 143
 - scopes (table), 140
 - Security Identifier (SID), 66, 96
 - security model, analyzing
 - current, 48
 - security patches, 18, 379
 - security planning, corporate
 - components of, 21–50
 - security plans, 2, 31, 182
 - security policy, planning, 22
 - Security Policy Template, 117
 - security principals, 66, 96
 - security risks
 - access to information, 3
 - access to network traffic, 4
 - external, 8
 - managing, 11–12
 - security templates
 - comparing current to previous system settings, 121
 - creating, 162, 250
 - default settings, 248–250
 - described, 117–120
 - secdit.exe tool, 124
 - securing servers using, 247–250
 - SMB signing, configuration, 271
 - security zones, 396, 405
 - server authentication, defined, 210
 - server configurations, evaluating
 - current, 49
 - Server Message Block (SMB) signing. *See* SMB signing
 - servers
 - configuring to use certificates, 191
 - DHCP. *See* DHCP servers
 - dial-up. *See* dial-up servers
 - proxy. *See* proxy servers
 - RIS, setting up, 232
 - securing using security templates, 247
 - Service Record, 221, 257
 - Services for Netware, 253
 - session key data encryption, 171, 209
 - session tickets
 - authentication process, 60
 - defined, 96
 - sex, controlling content, 399
 - shared folders
 - creating, 71, 102
 - default properties, 72
 - Shared Folder snap-in, 73
 - shared secrets
 - described, 58
 - Kerberos use of, 63
 - share permissions
 - combining with NTFS permissions, 77
 - defined, 96
 - in Windows 2000 (table), 71
 - Shiva Password Authentication Protocol (SPAP), 310
 - SIDs (Security Identifiers)
 - defined, 96
 - and security principals, 66
 - Simple Message Transfer Protocol. *See* SMTP
 - Simple Network Management Protocol. *See* SNMP
 - smart cards
 - described, 58
 - use described, 180
 - SMB signing
 - defined, 288
 - process described, 266
 - security options, 271
 - Windows 2000 Group Policy, 270
-

- SMTP (Simple Message Transfer Protocol)
 - clear text, and security risks, 4, 10
 - defined, 13
 - Smurf program, 7
 - snap-ins
 - IP Security, 284
 - Security Templates on MMC, 118
 - Shared Folder, 73
 - SNMP (Simple Network Management Protocol)
 - agents, 244, 257
 - authorized management solutions, 246
 - communities, 245–246, 257
 - described, 220, 244, 257
 - implementing security, 244–247
 - installing service, 246
 - management station defined, 257
 - securing transmissions, 247
 - traps, 244, 257
 - social engineering attacks, 9, 13, 315–316, 332
 - Southdale Property Management.
 - See* case projects
 - SPAP (Shiva Password Authentication Protocol), 310
 - SQL, domain administrator training, 6
 - SRV Record
 - defined, 257
 - described, 221
 - SSL (Secure Socket Layer)
 - configuring Web server to require (fig.), 195
 - defined, 209
 - handshake defined, 210
 - SSL handshake, 178
 - standalone CA, 185
 - standard primary zone, 257
 - standard secondary zone, 257
 - static mappings, 388, 389
 - static routes, 350, 370
 - Structured Query Language (SQL), 6
 - subordinate CAs, 175
 - subordinate enterprise CA, 185
 - subscribing, Microsoft Security Notification Service, 18
 - symmetric key, 210
 - System Access Control Lists (SACLs), 67, 96
 - T**
 - taskpads, 131, 133
 - tasks, delegating, 130–131
 - TCP/IP
 - advanced properties (fig.), 226
 - and DHCP, 224
 - Telnet, 394
 - templates
 - certificate, in Windows 2000 (table), 187
 - Group Policy, 146
 - security. *See* security templates
 - terminal servers, limiting access to, 241
 - Terminal Services
 - choosing mode (fig.), 240
 - described, 238–239, 257
 - installing, 239, 262
 - User group, 242
 - testing account policies, 164
 - TFTP (Trivial File Transfer Protocol), 238
 - TGT (Ticket Granting Ticket)
 - authentication process, 59
 - defined, 96
 - Thawte CA, 174
 - theft of computers, 3
 - third-party CAs, integration with, 205
 - three-horned firewall DMZ
 - defined, 405
 - Ticket Granting Ticket, 59, 96
 - time-of-day constraints, remote access policy (fig.), 320
 - TKEY negotiation, 229
 - TLS (Transport Layer Security), 178, 209
 - tools
 - Apcompat.exe utility, 249
 - Gpresult utility, 154
 - IAS administration, 327
 - Routing and Remote Access administration, 297
 - Security Configuration and Analysis utility, 121
 - security template, 124
 - UNIX secure access, 251
 - transitive trusts defined, 157
 - transmission security, 243–244
 - Transport Layer Security (TLS), 178, 209
 - Transport mode, IPSec, 275, 289
 - traps, SNMP, 244
 - Trivial File Transfer Protocol (TFTP), 238
 - Trojan Horses, 393
 - troubleshooting Group Policy settings, 154
 - trusted Web sites, 397
 - trust paths
 - checking out CAs, 175
 - creating, 184
 - defined, 210
 - in PKI (fig.), 177
 - Tunnel mode, IPSec, 276, 289
 - U**
 - unauthorized file downloads, 393
 - Universal groups defined, 157
 - universal principal name (UPN), 199
 - UNIX clients, securing network access to, 251
 - UPN (universal principal name), 199
 - user accounts
 - Active Directory's use of, 170
-

- configuring callback options (fig.), 313
 - creating for VPN connection, 336
 - mapping to certificates, 199–201
 - RAS policy testing, 338
 - remote access administration, 316
 - testing VPN server connection, 337
 - user authentication, implementing, 58–65
- V**
- Verisign CA, 174, 179
 - viewing event logs, 89
 - violence, controlling content, 399
 - virtual private network. *See* VPN
 - virtual tunnels, 342
 - viruses
 - Code Red Worm, 379
 - e-mail, 7, 380
 - Internet access, 393
 - VPN (virtual private network)
 - client configuration, 307
 - configuring, securing, 360–365
 - creating connection (fig.), 304
 - defined, 332, 370
 - implementing access, 302–304
 - server configuration, 305–306
 - tunneling protocol options, 361–365
- W**
- WAN (wide area network)
 - defined, 370
 - denial-of-service attacks and, 7
 - described, 342
 - linked corporate locations (fig.), 343
 - network diagram sample (fig.), 43
 - Web servers, configuring to require SSL (fig.), 195
 - Web Site Properties, Directory Security tab (fig.), 192
 - Web sites, secure, 178
 - Web usage reports, 390
 - wide area network. *See* WAN
 - Windows 2000
 - audit categories (fig.), 86, 88
 - configuring as router, 345
 - and IPSec, 277
 - networks, accessing resources on, 65–70
 - Registry, securing, 82
 - router, securing, 357
 - security holes in, 48
 - share permissions (fig.), 71
 - Windows 2000 Certificate Server, certificates available, default (fig.), 187
 - Windows 2000 Professional, built-in groups, 141
 - Windows 2000 servers, securing resources on, 57–95
 - Windows 95, file-level security, 3
 - Windows 98
 - file-level security, 3
 - SMB signing, editing Registry, 268
 - Windows 9x
 - DHCP server registration, 228, 230
 - Terminal Services client, 239
 - Windows Internet Naming Service (WINS), 44
 - Windows NT
 - administrative task delegation, 128
 - DHCP server registration, 228, 230
 - inadequacy of network security, 116
 - SMB signing, editing Registry, 268
 - Terminal Services client, 239
 - vs. Windows 2000 Active Directory, 40
 - Windows NT domains, access to administrative rights, 5
 - WINS (Windows Internet Naming Service), 44
 - wizards
 - Add New Hardware, 296
 - Create Shared Folder, 73
 - Delegation of Administration, 138
 - Delegation of Control, 131
 - Demand Dial Interface (fig.), 354–356
 - IIS Certificate (fig.), 193, 194
 - Network Connection, 301
 - RRAS Setup, 346
- X**
- X.25 connections, 296
 - X.509 Version 3, 173, 210
- Z**
- zone transfer defined, 257
 - zones, DNS. *See* DNS zones
-